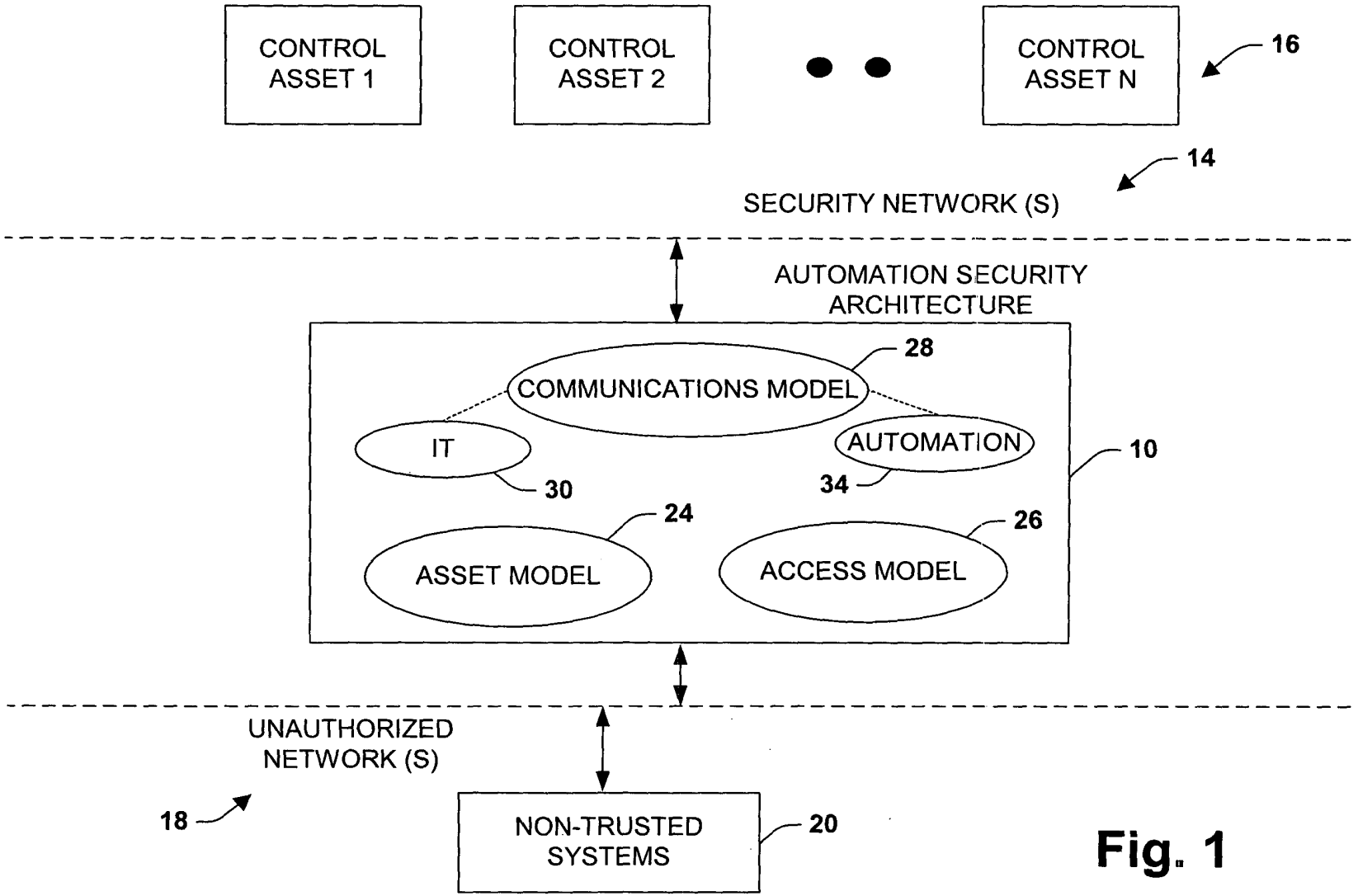
CONTROL ASSET 1
CONTROL ASSET 2
CONTROL ASSET N
16
14
SECURITY NETWORK (S)
AUTOMATION SECURITY ARCHITECTURE
28
COMMUNICATIONS MODEL
IT
30
AUTOMATION
34
10
24
ASSET MODEL
26
ACCESS MODEL
UNAUTHORIZED NETWORK (S)
18
NON-TRUSTED SYSTEMS
20

Fig. 1

Actor / Role	Asset	Access
Integrator	Line, Machine	R/W
OEM	Machine	R/W
Supplier	Component	R/W
Local Maintenance	Factory, Line	R/W
Outsourced Monitoring	Component	RO
Management	Line, Machine	RO
Engineering	Line, Machine	R/W

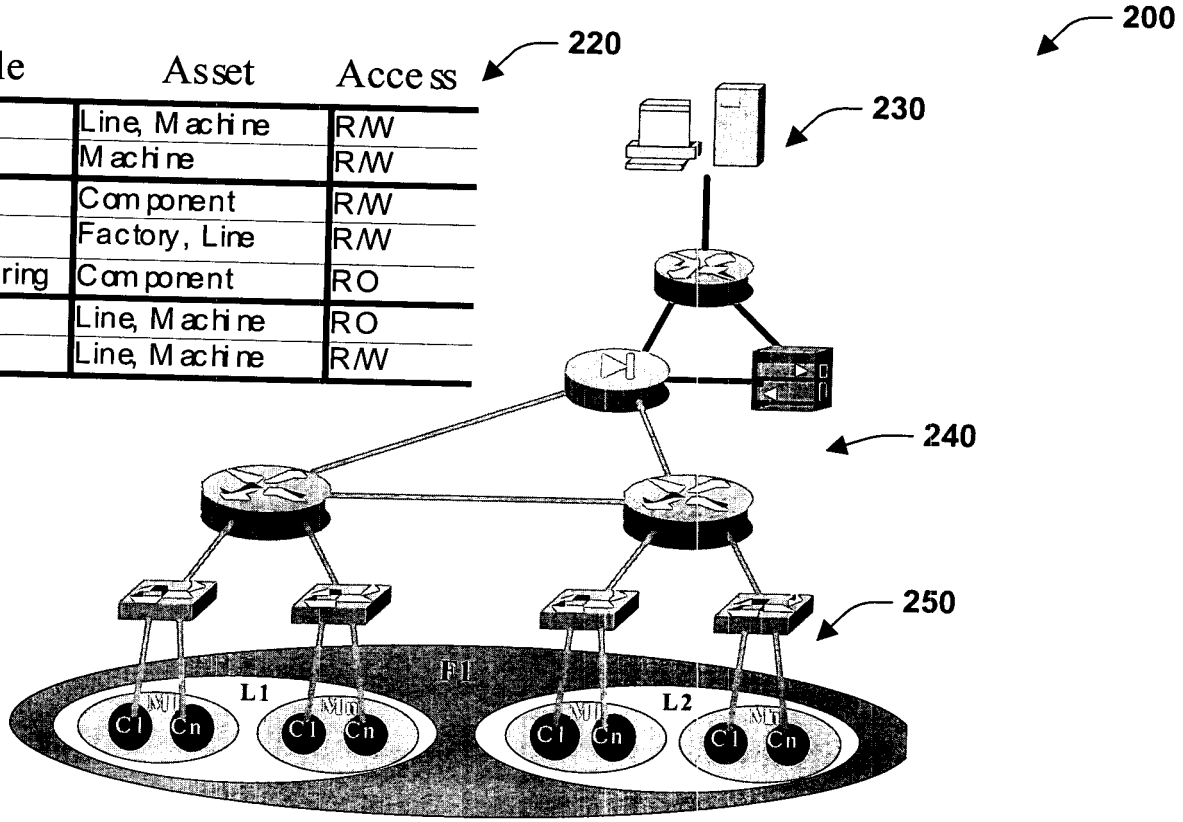

Fig. 2

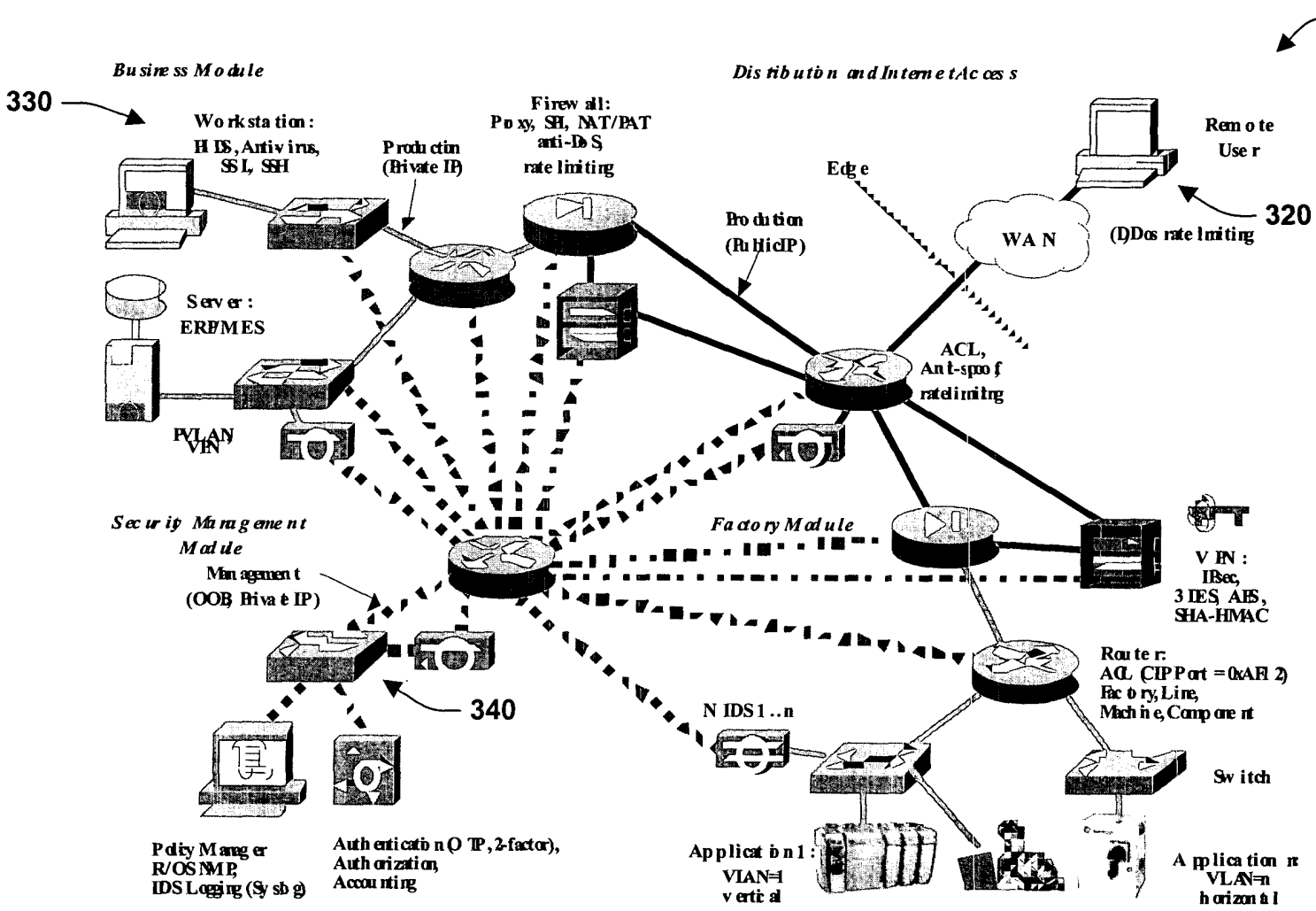
300
Business Module
330
Distribution and Internet Access
Workstation:
HIDS, Antivirus,
SSL, SSH
Productin
(Private IP)
Firewall:
Proxy, SH, NAT/PAT
anti-DoS,
rate limiting
Edge
Remote
User
320
Production
(PublicIP)
WAN
(D)Dos rate limiting
Server:
ERP/MES
ACL,
Anti-spoof
ratelimitng
PVLAN
VIN
Security Management
Module
Factory Module
Management
(OOB, Private IP)
VPN:
IPSec,
3DES, AES,
SHA-HMAC
Router:
ACL, CIPPort = 0xAF12
Factory, Line,
Machine, Component
340
NIDS1..n
Switch
Policy Manager
R/OS NMP,
IDS Logging (Syslog)
Authentication (OTP, 2-factor),
Authorization,
Accounting
Application:
VLAN=1
vertical
Application
VLAN=n
horizontal
310

Fig. 3

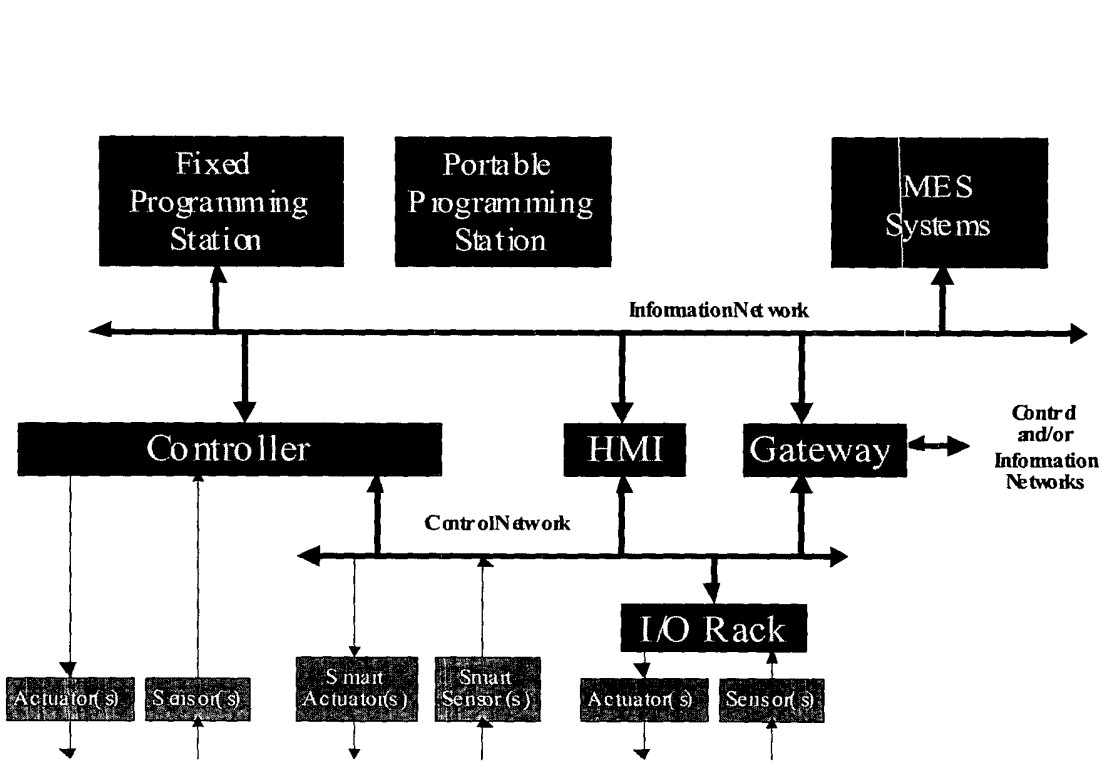
400
Fixed Programming Station
Portable Programming Station
MES Systems
InformationNetwork
Controller
HMI
Gateway
Contrd and/or Information Networks
ControlNetwork
I/O Rack
Actuator(s)
Sensor(s)
Smart Actuator(s)
Smart Sensor(s)
Actuator(s)
Sensor(s)

Fig. 4

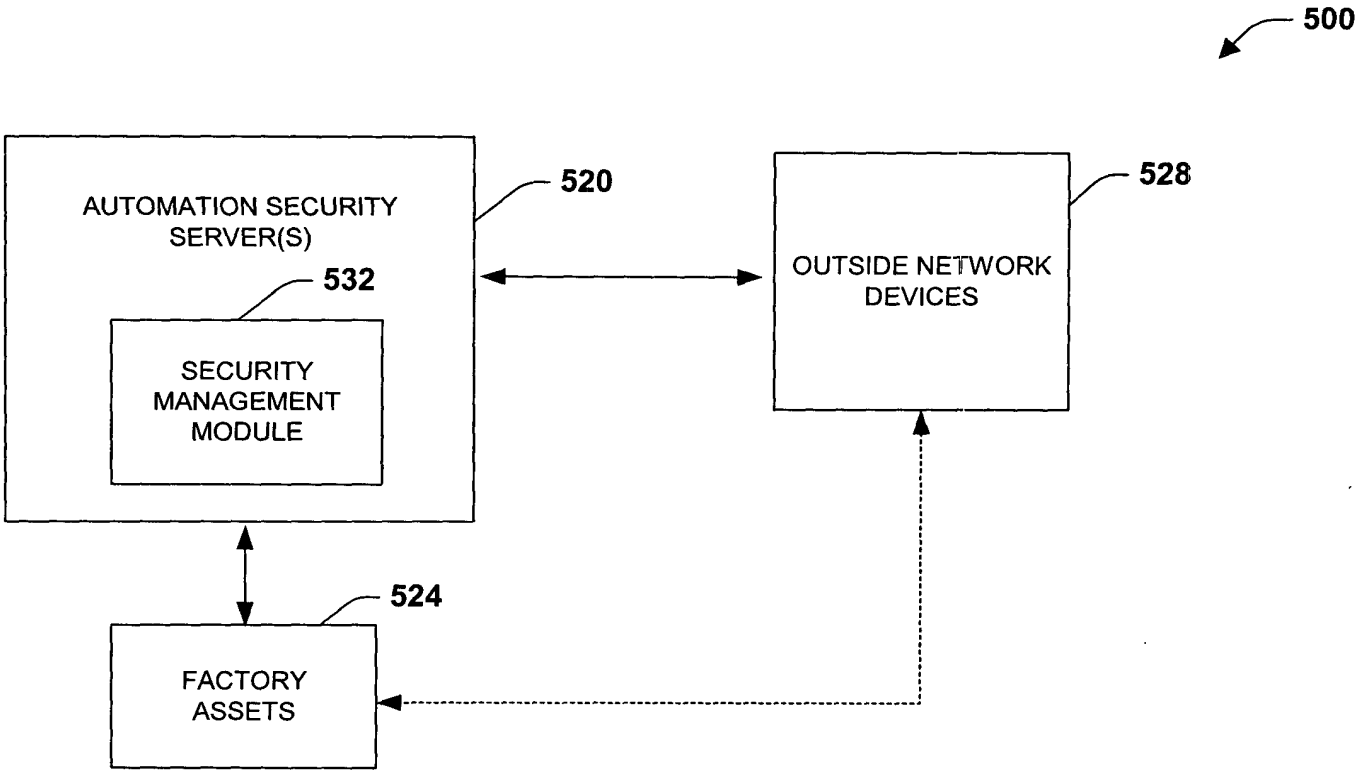
500
AUTOMATION SECURITY SERVER(S)
520
532
SECURITY MANAGEMENT MODULE
OUTSIDE NETWORK DEVICES
528
524
FACTORY ASSETS

Fig. 5

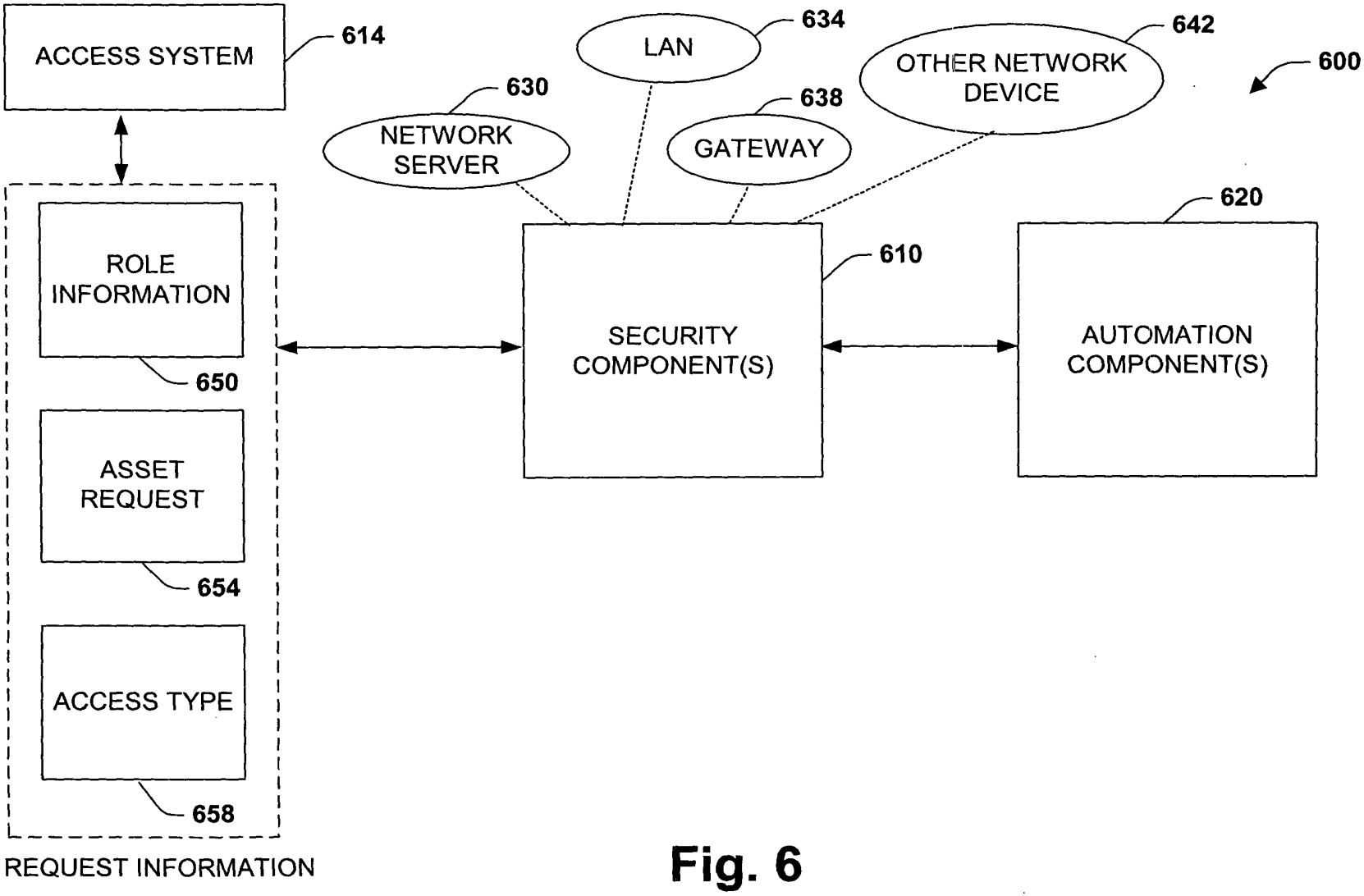
ACCESS SYSTEM
614
LAN
634
OTHER NETWORK DEVICE
642
600
630
NETWORK SERVER
638
GATEWAY
620
610
ROLE INFORMATION
650
SECURITY COMPONENT(S)
AUTOMATION COMPONENT(S)
ASSET REQUEST
654
ACCESS TYPE
658
REQUEST INFORMATION

Fig. 6

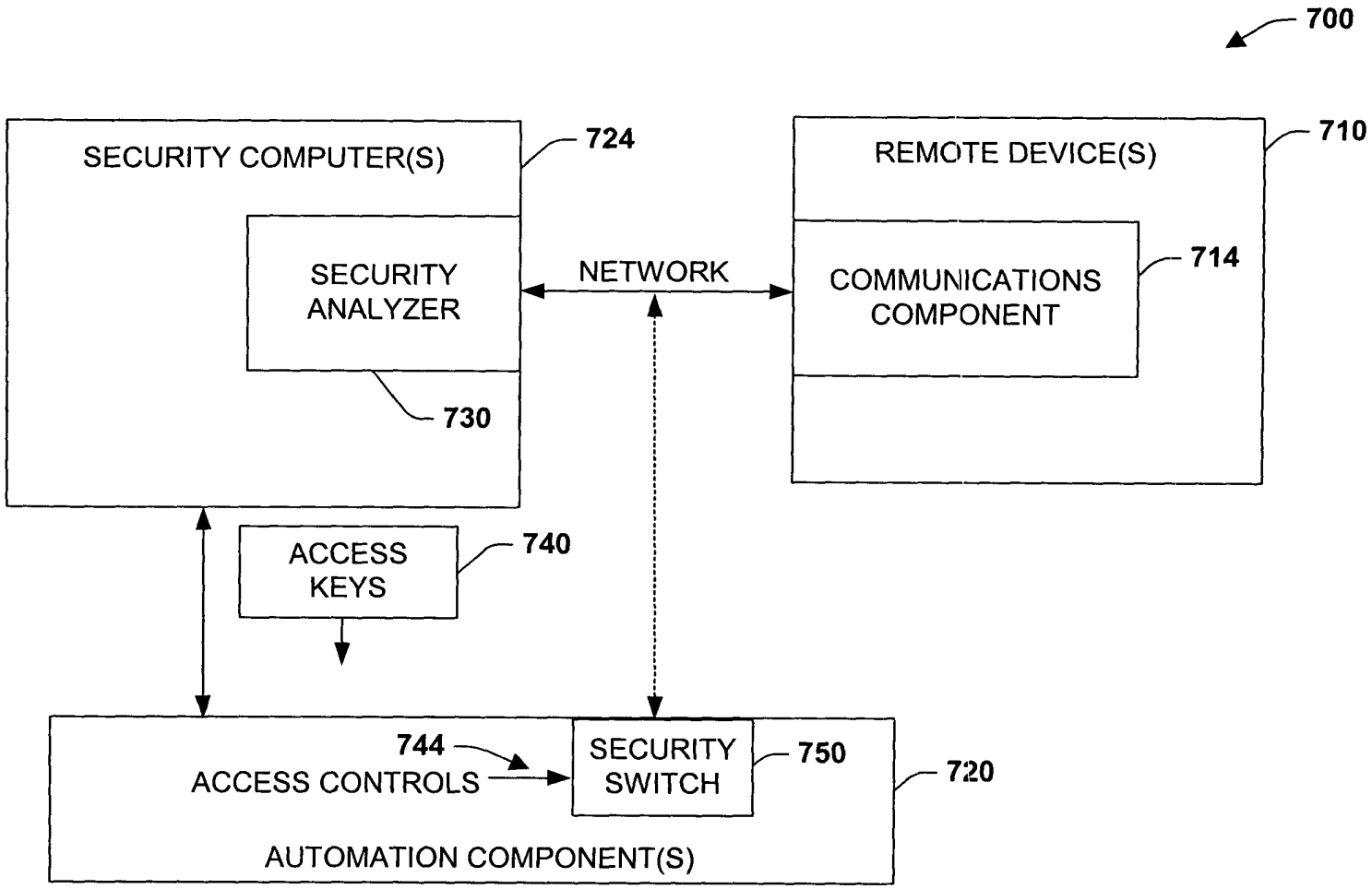
700
SECURITY COMPUTER(S)
724
SECURITY ANALYZER
730
NETWORK
REMOTE DEVICE(S)
710
COMMUNICATIONS COMPONENT
714
ACCESS KEYS
740
744
ACCESS CONTROLS
SECURITY SWITCH
750
720
AUTOMATION COMPONENT(S)

Fig. 7

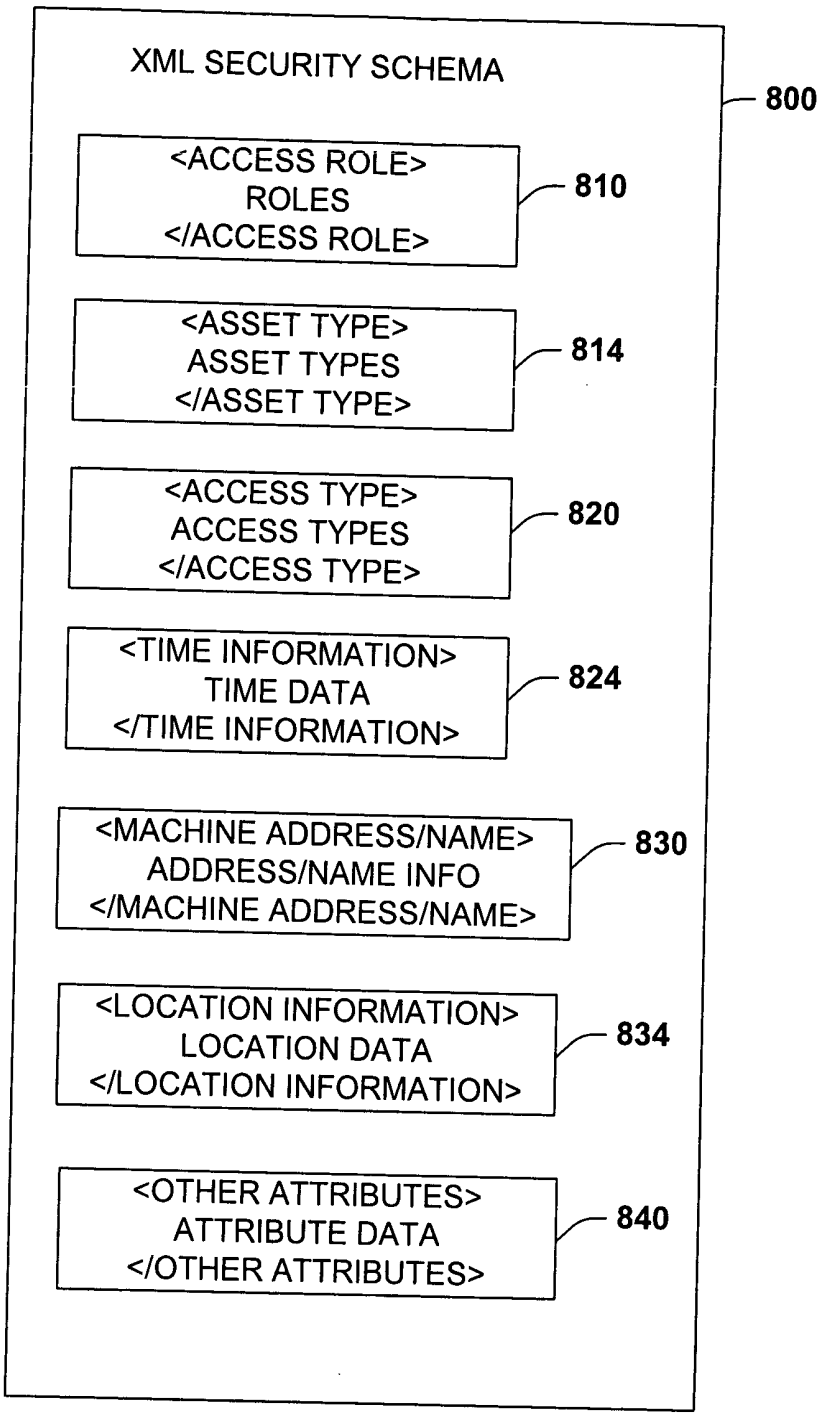
XML SECURITY SCHEMA
800
<ACCESS ROLE>
ROLES
</ACCESS ROLE>
810
<ASSET TYPE>
ASSET TYPES
</ASSET TYPE>
814
<ACCESS TYPE>
ACCESS TYPES
</ACCESS TYPE>
820
<TIME INFORMATION>
TIME DATA
</TIME INFORMATION>
824
<MACHINE ADDRESS/NAME>
ADDRESS/NAME INFO
</MACHINE ADDRESS/NAME>
830
<LOCATION INFORMATION>
LOCATION DATA
</LOCATION INFORMATION>
834
<OTHER ATTRIBUTES>
ATTRIBUTE DATA
</OTHER ATTRIBUTES>
840

Fig. 8

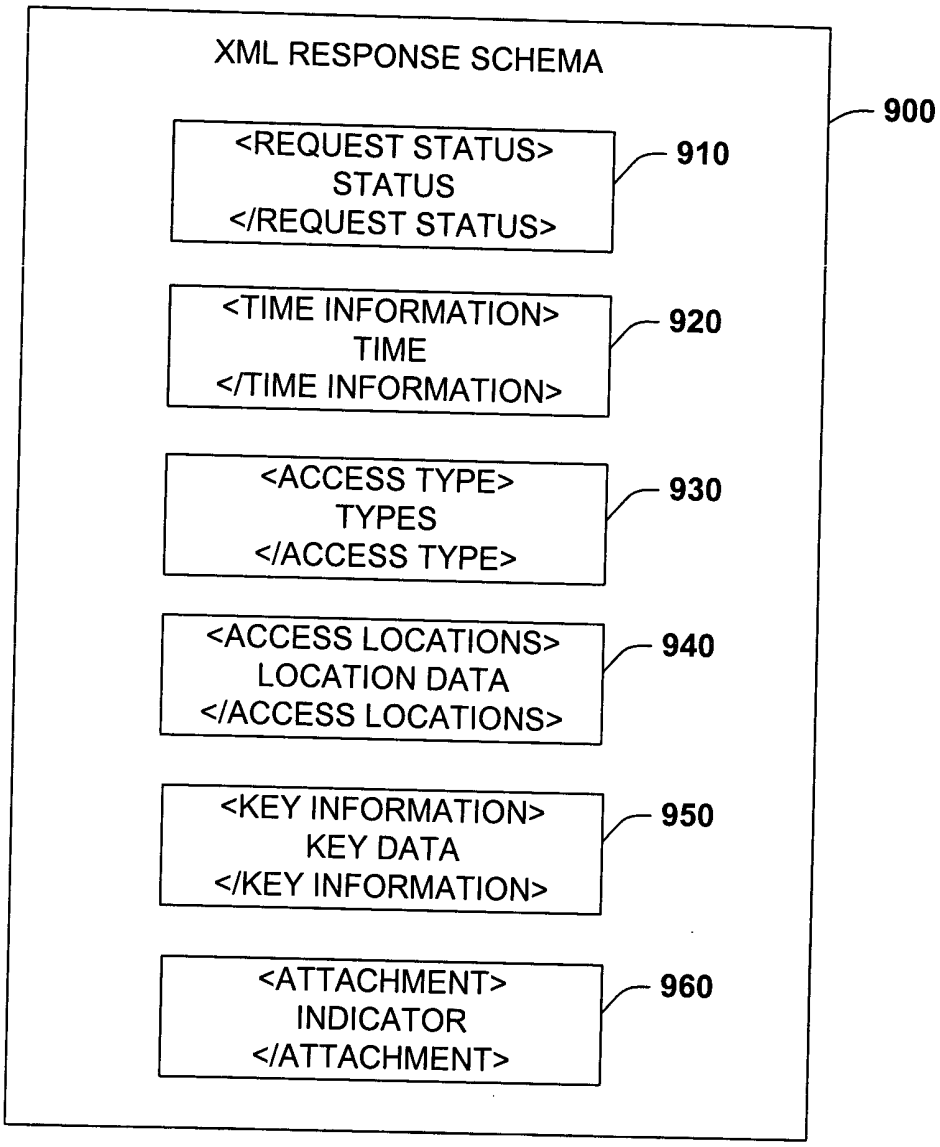
XML RESPONSE SCHEMA
900
<REQUEST STATUS>
STATUS
</REQUEST STATUS>
910
<TIME INFORMATION>
TIME
</TIME INFORMATION>
920
<ACCESS TYPE>
TYPES
</ACCESS TYPE>
930
<ACCESS LOCATIONS>
LOCATION DATA
</ACCESS LOCATIONS>
940
<KEY INFORMATION>
KEY DATA
</KEY INFORMATION>
950
<ATTACHMENT>
INDICATOR
</ATTACHMENT>
960

Fig. 9

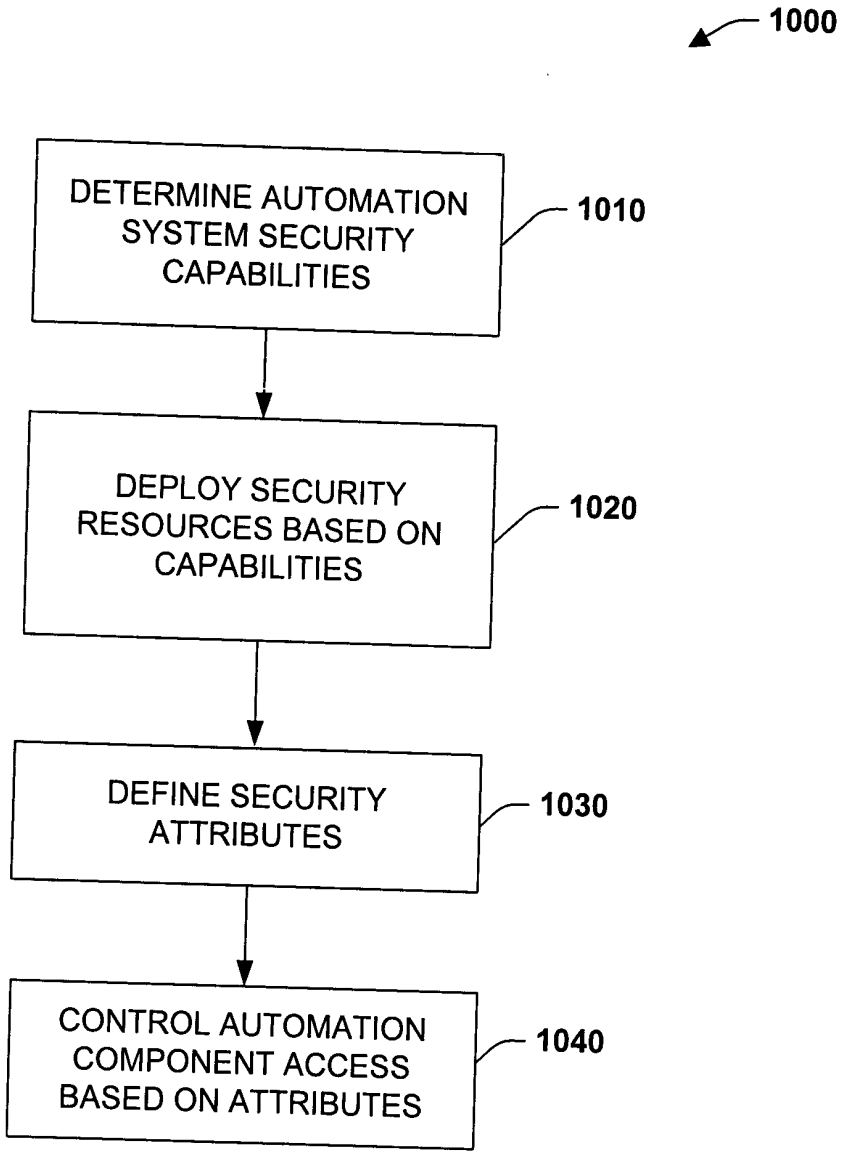
1000
DETERMINE AUTOMATION SYSTEM SECURITY CAPABILITIES
1010
DEPLOY SECURITY RESOURCES BASED ON CAPABILITIES
1020
DEFINE SECURITY ATTRIBUTES
1030
CONTROL AUTOMATION COMPONENT ACCESS BASED ON ATTRIBUTES
1040

Fig. 10

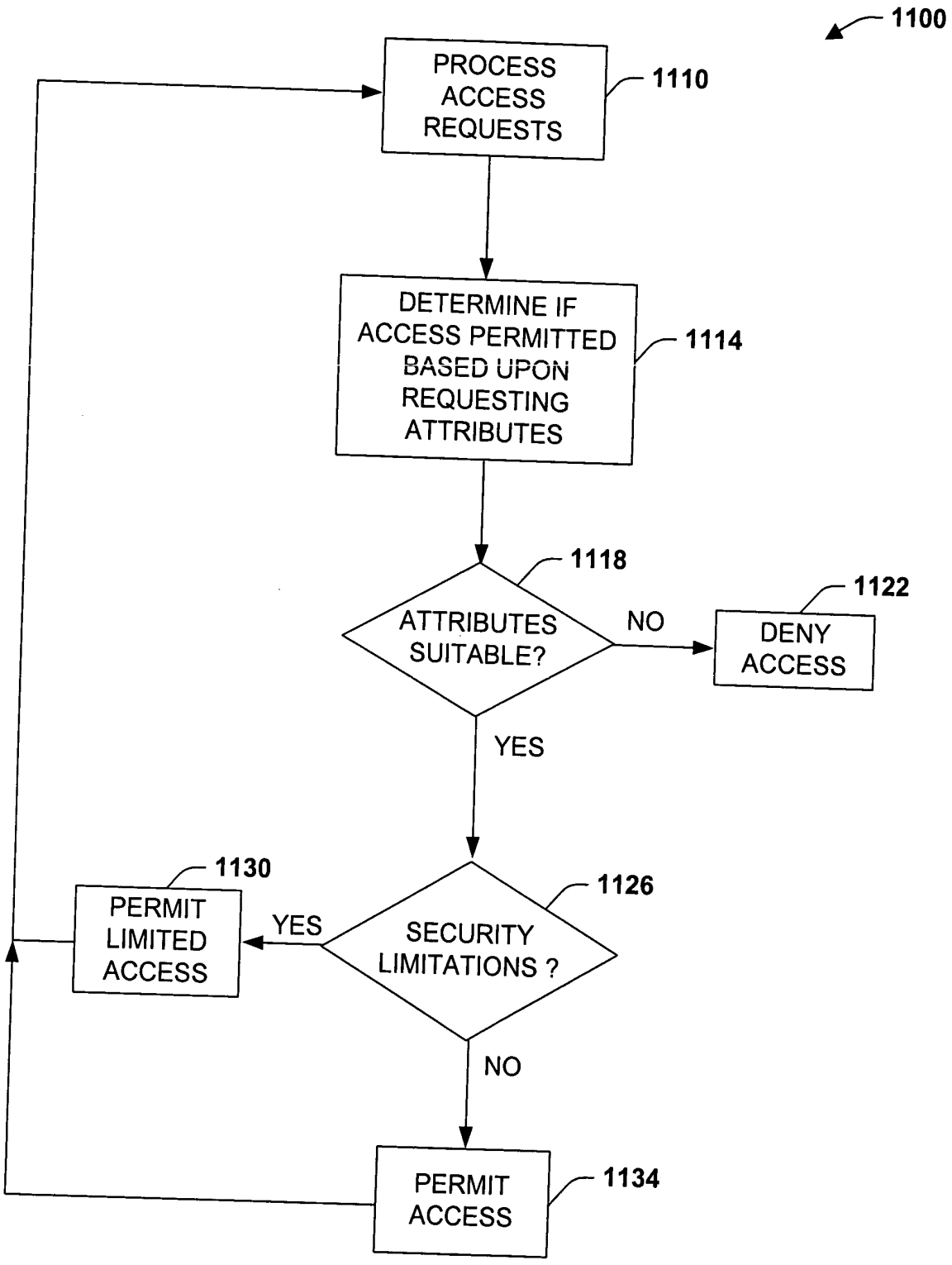
1100
PROCESS ACCESS REQUESTS
1110
DETERMINE IF ACCESS PERMITTED BASED UPON REQUESTING ATTRIBUTES
1114
1118
ATTRIBUTES SUITABLE?
NO
1122
DENY ACCESS
YES
1126
SECURITY LIMITATIONS ?
YES
1130
PERMIT LIMITED ACCESS
NO
PERMIT ACCESS
1134

Fig. 11